(12) PATENT
(19) AUSTRALIAN PATENT OFFICE

(11) Application No. AU 199712449 B2
(10) Patent No. 707125

(54) Title
Electronic access control and security system

(51)[6] International Patent Classification(s)
G08B 013/00 E05B 047/02
E05B 047/00 H04M 011/04

(21) Application No: 199712449 (22) Application Date: 1997.02.03

(30) Priority Data

(31) Number	(32) Date	(33) Country
19609319	1996.03.09	DE

(43) Publication Date : 1997.09.11
(43) Publication Journal Date : 1997.09.11
(44) Accepted Journal Date : 1999.07.01

(71) Applicant(s)
Krone Aktiengesellschaft

(72) Inventor(s)
Wolfgang Kraft; Andries Kortland

(74) Agent/Attorney
DAVIES COLLISON CAVE,1 Little Collins Street,MELBOURNE VIC 3000

(56) Related Art
DE 4302835

US 4882752

AU9712449

(12) PATENT ABSTRACT (11) Document No. AU-A-12449/97
(19) AUSTRALIAN PATENT OFFICE

(54) Title
ELECTRONIC ACCESS CONTROL AND SECURITY SYSTEM

International Patent Classification(s)
(51)[6] G08B 013/00 E05B 047/00 E05B 047/02 H04M 011/04

(21) Application No. : 12449/97 (22) Application Date : 03/02/97

(30) Priority Data

(31) Number	(32) Date	(33) Country
19609319	09/03/96	DE GERMANY

(43) Publication Date : 11/09/97

(71) Applicant(s)
KRONE AKTIENGESELLSCHAFT

(72) Inventor(s)
WOLFGANG KRAFT; ANDRIES KORTLAND

(74) Attorney or Agent
DAVIES COLLISON CAVE , 1 Little Collins Street, MELBOURNE VIC 3000

(57) The invention relates to an electronic access control and security system against unauthorised opening of closed objects, in particular control and distribution cabinets of the communication and data technique, according to the preamble of claim 1.

The object of the present invention, namely to provide an electronic access control and security system, by means of which the security against unauthorised opening is further improved and an always up-to-date information about the condition of the object to be protected is secured, is achieved by that within a multi-stage hierarchy the central control unit (CCU) is connected by at least one decentral communication multiplexer (DCM) to at least one local data processor (LDP), decentral communication multiplexer (DCM) and local data processor (LDP) being adapted as semi-autonomous electronic units, and local data processor (LDP) being installed in the object respectively to be protected, and between the object to be protected and central control unit (CCU) a continuously up-dated data exchange by a dynamic protocol about the condition of the object and access attempts or the like being performed, power supply of local data processor (LDP) and communication taking place over the same 2-wire connection. - Fig. 1 -.

CLAIM

1. A electronic access control and security system against unauthorised opening of closed objects, in particular control and distribution cabinets of the communication and data technique, comprising a central data acquisition

.../2

and a computer-aided central data evaluation and a remote data transmission over the communication and data cable, a communication device for identification control and access authorisation, characterised in that within a multi-stage hierarchy the central control unit (CCU) is connected by at least one decentral communication multiplexer (DCM) to at least one local data processor (LDP), decentral communication multiplexer (DCM) and local data processor (LDP) being adapted as semi-autonomous electronic units, and local data processor (LDP) being installed in the object respectively to be protected, and between the object to be protected and central control unit (CCU) a continuously up-dated data exchange by a dynamic protocol about the condition of the object and access attempts or the like being performed, power supply of local data processor (LDP) and communication taking place over the same 2-wire connection.

AUSTRALIA

PATENTS ACT 1990

COMPLETE SPECIFICATION

NAME OF APPLICANT(S):

Krone Aktiengesellschaft

ADDRESS FOR SERVICE:

DAVIES COLLISON CAVE
Patent Attorneys
1 Little Collins Street, Melbourne, 3000.

INVENTION TITLE:

Electronic access control and security system

The following statement is a full description of this invention, including the best method of performing it known to me/us:–

The invention relates to an electronic access control and security system against unauthorised opening of closed objects, in particular control and distribution cabinets of the communication and data technique, according to the preamble of claim 1.

Protection against unauthorised use of telecommunication paths is becoming more and more important, in order to prevent monitoring of private and commercial lines, performing telephone calls on somebody else's cost and to make manipulations of data and deliberate damaging more difficult.

From DE 43 02 835 C1 is known in the art a mechanical closing device for the door of a housing, in particular a cable junction box of the communication and data technique, wherein a locking device with two actuation stages for a locking bar is provided. After displacing the bar into its first actuation stage, an opening comes free. The authorised person can have access through this opening to plug bushings or a magnetic card reader or the like and connect a communication device. By means of the communication de-

vice the authorised person can make contact to a control centre and effect release of the second actuation stage. The exchange of information between centre and authorised person at the cable junction box serves for identification control.

By this prior art closing device, security against unauthorised use is considerably improved, an always up-to-date control of the condition of the complete cable junction box and the persons asking for access is however not secured.

It is the object of the present invention to provide an electronic access control and security system of the type referred to hereinbefore, by means of which the security against unauthorised opening is further improved and an always up-to-date information about the condition of the object to be protected is secured.

This object is achieved by the features of claim 1.

By distributing the computer capacity to three hierarchies it is achieved that computer capacity is installed also in the object to be protected, whereby an analysis of events in and at the object can be performed (decentral intelligence).

Whereas in prior art security systems only the general signalisation of events to a centre is provided, it will be signalled, according to the invention, what has happened where and when. The continuous monitoring and up-dating of the signals (data) in a dialogue between the decentral communication multiplexers (DCM), the local data processors (LDP) and the central communication unit (CCU) with the use of a dynamic protocol to the actual condition of the object secure that a higher security against unauthorised opening, an identification of opening attempts and also of attempts to interrupt the lines, of burglary attempts or the like is achieved. Each failure is identified as such, there is a very high reliability of the system. Not only the door, but the complete object is protected from burglary or sabotage.

Protection of a large assembly of installations with a big number of keys is possible. Assignment of the keys can be limited in time, for a certain section of the assembly of installations and also to combined place/time criteria. Each key number is world-wide only once available. Modifi-

cations of authorisations can only be performed at the central communication unit by an authorisation terminal.

The electronic key can be selected in a pin or magnetic card form.

Access to an object is always secured for an authorised user, even when there is a power failure. Power supply is provided for the electronic lock by the DCM. The mechanical lock can be opened by the authorised user even in case of a power failure, the mechanical lock remains operable.

There is an automatic up-date of the access criteria over all levels. The central administration and control by the central communication unit provides clear structuring, actuality and effective handling possibilities.

In the following, the invention will be described in more detail, based on an embodiment of an electronic access control and security system shown in the drawings. There are:

Fig. 1 the system survey,

Fig. 2 the diagrammatical representation of the assemblies and components of the LDP on the inner door side of the cable junction box.

The electronic access control and security system according to the representation of Fig. 1 is installed for the protection of a multitude of cable junction boxes 1 and combined with the two-stage mechanical closing system respectively present in cable junction box 1, for example according to DE-43 02 835 C1 (not shown).

According to Fig. 1, the system is composed of a central control unit CCU connected to a decentral communication multiplexer DCM, and of a multitude of local data processors LDP in cable junction boxes 1 each connected by a 2-wire cable 2 and a main distribution box HVT to the decentral communication multiplexer DCM.

Main distribution box HVT can for example be replaced by floor distribution boxes in building networks, if a main distribution box is not needed.

In door 3 of respective cable junction box 1 is disposed, not visible from outside, local data processor LDP as an electronic monitoring unit working in conjunction with the two-stage mechanical closing unit. Local data

processor LDP serves for the status control of cable junction box 1 and monitors door 3 with regard to door position, locking bar position, locking bar blocking, monitors the complete cable junction box 1 with regard to sabotage attempts. Local data processor LDP includes according to Fig. 2 an identification reader 14 for the "electronic key". The electronic key can be configured in the form of a magnetic card or of a pin structure. Local data processor LDP includes a computer module 12 with a CPU and a storage capacity. Local data processor LDP processes all signal coming from sensors, such as light sensor 15, open/closed sensor 16, to specific coded messages, it monitors all accesses/openings or opening attempts and sabotage actions by a sabotage switch S. Local data processor LDP communicates by a cable 4 (1-DW cable) with decentral communication multiplexer DCM.

The mechanical arrangement of the elements can be varying, depending on the object to be protected.

In case of a failure of the power supply of the local data processors LDP, for instance by a damage to the communication cable during earthworks, the monitoring section of the local data processors LDP will continue to operate for several hours and records and stores status modifications of box 1 during that time. After power is back, the data are automatically transmitted to central control unit CCU.

Decentral communication multiplexer DCM secures the power supply of local data processor LDP over cable 4 and also the data exchange by coded protocols; it is the interface between local data processors LDP and central control unit CCU (central computer). It monitors all local data processors LDP, with the possibility that a main distribution box HVT is interposed between local data processors LDP and decentral communication multiplexer DCM.

In Fig. 1 is shown the monitoring section of a decentral communication multiplexer DCM; however a multitude of such monitoring sections can be combined, so that several decentral communication multiplexers DCM can be connected to a central control unit CCU.

Central control unit CCU handles the central communication of all decentral communication multiplexers DCM and includes the network file, the authorisation file (access authorisations as a numerically sorted key list and an up-

dated list) for the electronic key and for statistical evaluations. An alarm is recognised and initiated in central control unit CCU. From central control unit CCU, information can be directed to selected receivers.

Access to a cable junction box 1 or the opening thereof is allowed by that the authorised person releases the first locking of the lock by means of the mechanical key, and makes accessible thereby a not shown opening into which is inserted a not shown coded electronic key, or as in another embodiment, where he approaches a coded identification means for non-contact reading.

After identification, and thus authorisation for opening door 3 of cable junction box 1 is accomplished, the second electronically secured locking is released; the door can be opened by the authorised person.

According to Fig. 2, the electronic key is detected by the proximity antenna 5, and the data detected are forwarded to computer module 12 of local data processor LDP for further evaluation. In computer module 12 is checked whether the key is authorised for opening cable junction box 1. The detected authorisation for opening is transmitted over modem 6 to decentral communication multiplexer DCM. From there the signal is conducted over computer module 12 to booster 13, and holding solenoid is 7 de-activated. The mechanical arrangement of the elements can be varying, depending on the object to be secured.

If the authorised person does not open door 3 of cable junction box 1 within a specified time, for example 30 seconds, holding solenoid 7 and thus electronic locking 11 of the lock is re-activated.

L E G E N D

01	box
02	2-wire cable
03	door
04	cable
05	antenna
06	modem
07	holding solenoid
08	sabotage switch
09	sensor circuitry
10	locking control
11	LDP locking
12	computer module
13	booster
14	identification reader
15	light sensor
16	open/closed sensor

HVT	main distribution box
CCU	central control unit
DCM	decentral multiplexer module
LDP	local data processor

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A electronic access control and security system against unauthorised opening of closed objects, in particular control and distribution cabinets of the communication and data technique, comprising a central data acquisition and a computer-aided central data evaluation and a remote data transmission over the communication and data cable, a communication device for identification control and access authorisation, characterised in that within a multi-stage hierarchy the central control unit (CCU) is connected by at least one decentral communication multiplexer (DCM) to at least one local data processor (LDP), decentral communication multiplexer (DCM) and local data processor (LDP) being adapted as semi-autonomous electronic units, and local data processor (LDP) being installed in the object respectively to be protected, and between the object to be protected and central control unit (CCU) a continuously up-dated data exchange by a dynamic protocol about the condition of the object and access attempts or the like being performed, power supply of local data processor (LDP) and communication taking place over the same 2-wire connection.

2. An electronic access control and security system according to claim 1, characterised in that various sensors in and/or at the object are provided for monitoring the complete object condition, the information of which is processed independently from each other in a local data processor (LDP) and transmitted as a concrete message over decentral communication multiplexer (DCM) to central control unit (CCU).

3. An electronic access control and security system according to claim 1, characterised in that respective local data processor (LDP) is positioned at the inner side of the object door, provided with an own electronic lock and connected to the mechanical closing device.

4. An electronic access control and security system according to claims 1 to 3, characterised in that the power supply secures the electronic locking of the object door and in case of a power failure, access by the authorised person is secured.

5. An electronic access control and security system according to claim 3, characterised in that for the access control of the object, a proximity reader is disposed as an identification system in local data processor (LDP), said reader checking an identification means provided outside.

6. An electronic access control and security system according to claims 1 to 5, characterised in that an identification number once assigned is used.

7. An electronic access control and security system according to claims 1 to 6, characterised in that access authorisation (key assignment) is limited in time.

8. An electronic access control and security system according to claims 1 to 7, characterised in that over local data processor (LDP) further sensors for remote control, temperature and/or humidity measurement or the like are connected.

9. An electronic access control and security system according to claims 1 to 8, characterised in that coupling to customised networks by suitable interfacing is provided.

10. An electronic access control and security system substantially as hereinbefore described with reference to the drawings and/or Examples.

DATED this 21st day of April, 1999

Krone Aktiengesellschaft

by DAVIES COLLISON CAVE
Patent Attorneys for the applicant(s)

A B S T R A C T

The invention relates to an electronic access control and security system against unauthorised opening of closed objects, in particular control and distribution cabinets of the communication and data technique, according to the preamble of claim 1.

The object of the present invention, namely to provide an electronic access control and security system, by means of which the security against unauthorised opening is further improved and an always up-to-date information about the condition of the object to be protected is secured, is achieved by that within a multi-stage hierarchy the central control unit (CCU) is connected by at least one decentral communication multiplexer (DCM) to at least one local data processor (LDP), decentral communication multiplexer (DCM) and local data processor (LDP) being adapted as semi-autonomous electronic units, and local data processor (LDP) being installed in the object respectively to be protected, and between the object to be protected and central control unit (CCU) a continuously up-dated data exchange by a dynamic protocol about the condition of the object and access attempts or the like being performed, power supply of local data processor (LDP) and communication taking place over the same 2-wire connection. - Fig. 1 -.

12449/97

FIG.1

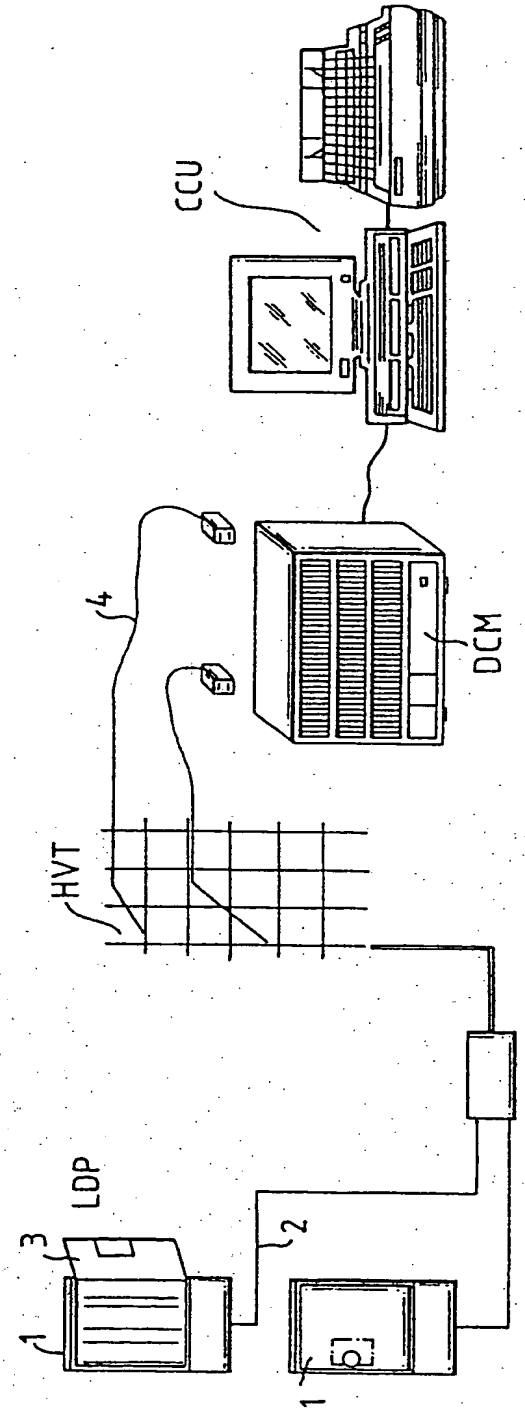

FIG.2